REMARKS

The Examiner is thanked for carefully considering the amended claims. By this amendment, Claims 1, 8, 9, 11, 13, 16, 17, 24, 25, 27, 29, 32, 33 and 40 have been amended. No claims have been added. Hence, Claims 1-40 are currently pending in the Application. It is respectfully submitted that the amendments to the claims as indicated herein do not add any new matter to this application.

CLAIM OBJECTIONS

Claims 8, 9, 24, 32, 40 have been objected to for various informalities. Claims 8, 9, 24, 32, 40 have been amended to correct these informalities.

REJECTIONS UNDER 35 U.S.C. § 112

Claims 8, 11, 13, 16, 24, 27, 29 and 32-40 have been rejected under 35 U:S.C. § 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 8, 11, 13, 16, 24, 27, 29 and 32-40 as amended are now in compliance with the requirements of 35 U.S.C. § 112, second paragraph.

REJECTIONS UNDER 35 U.S.C. § 102 and § 103

Claims 1-40 have been rejected under 35 U.S.C. Sections 102 and 103 respectively as being unpatentable over *Wasilewski et al.* (U.S. Patent 5,341,425), *Ng et al.* (U.S. Patent 5,581,614) and *Ganesan et al.* (U.S. Patent 5,588,061), either alone or in combination. Applicant respectfully submits that neither *Wasilewski* nor *Ganesan*, nor *Ng*, taken alone or in combination, discloses the method or apparatus as claimed in the amended independent claims 1, 9, 17, 25 and 33.

Neither *Wasilewski* nor *Ganesan*, nor *Ng*, taken alone or in combination, discloses "[A method including the steps:] …obtaining a first [encrypting/decrypting] key; generating a second [encrypting/decrypting] key as a function of the first [encrypting/decrypting] key and as a function of an identified parameter, "***wherein said identified parameter has a value; changing said value***;" [encrypting/decrypting] the data message "using the second [encrypting/decrypting] key to generate…a data message..." as claimed in independent claims 1, 9, 17, 25 and 33.

Neither *Wasilewski* nor *Ganesan*, nor *Ng*, taken alone or in combination, teaches using an encryption key to generate a second key with a function that changes. *Wasilewski* teaches a data transmission system comprising a plurality N of transmission sites and at least one reception site, a set of data at each transmission site is uniquely encrypted by (a) providing each transmission site with a broadcast key unique to that transmission site and a system key that is the same for all transmission sites, the system key comprising a plurality S of bits and each of the broadcast keys comprising a unique plurality B of bits, wherein B is less than S; (b) convolving in a predetermined manner at each transmission site the system key and the broadcast key unique to that transmission site to generate a unique data encryption key for that transmission site; (c) encrypting the set of data at each transmission site with the unique data encryption key generated at that site.. *Ganesan* teaches a method for improving an RSA cryptosystem by generating a user private exponent key, having an associated modulus N, and a user public exponent key for each user of the system. *Ng* teaches a decrypting method including the steps of reading a current month from a clock, extracting an odd/even month indication from the header portion, generating a first key based on the current month if the odd/even indication is odd and the current month is odd or if the odd/even indication is even and the current month is even, otherwise generating the first key based on a month previous to the current month read from the clock if the odd/even indication is odd and the current month is even or if the odd/even indication is even and the current month is odd, and using the first key for decrypting the encrypted body portion to generate a decrypted body portion. None of the cited references disclose the method of the present invention. There is no suggestion to apply *Ng* to the methods of *Wasilewski* or *Ganesan*, nor would such a combination function.

Thus, Amended Claims 1, 9, 17, 25 and 33 contain limitations that are not suggested by either *Wasilewski* or *Ganesan*, or *Ng*, either taken alone or in combination. Therefore, based on the reasons stated herein, it is respectfully submitted that Claims 1, 9, 17, 25 and 33 are allowable over the art of record and that Claims 1, 9, 17, 25 and 33 be held in condition for allowance.

Claims 2-8, 10-16, 18-24, 26-32 and 34-40 depend from claims 1, 9, 17, 25 and 33, respectively and are therefore also allowable over the art of record and should be held in condition for allowance.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

If in the opinion of the Examiner a telephone conference would expedite the prosecution of the subject application, the Examiner is encouraged to call the undersigned at (510) 252-4417.

Respectfully submitted,

Date: February 6, 2005

Tamiz Khan
Registration No. 46,273

Correspondence Address:

Tamiz Khan, Esq.
Prediwave Corp.
48431 Milmont Drive,
Fremont, California 94538
(510) 252-4417

VERSION OF CLAIMS WITH MARKINGS TO SHOW CHANGES MADE

1. (Once Amended) A method for securely transmitting a data message, comprising the steps of: obtaining a first encrypting key; generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter, wherein said identified parameter has a value; changing said value; encrypting the data message using the second encrypting key to generate an encrypted data message; and transmitting the encrypted data message.

2. The method of claim 1, wherein the encrypting step corresponds to a public key encryption scheme.

3. The method of claim 2, wherein the encryption scheme is an RSA scheme.

4. The method of claim 1, wherein the encrypting step corresponds to a private key encryption scheme.

5. The method of claim 4, wherein the encryption scheme is a DES scheme.

6. The method of claim 1, wherein the identified parameter is a time or time-dependent value.

7. The method of claim 1, wherein the identified parameter is a randomly generated number.

8. (Once Amended) The method of claim 1, further comprising: receiving the encrypted data message; obtaining a first [decryption] decrypting key; generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter; and decrypting the encrypted data message using the second decrypting key to recover the data message.

9. (Once Amended) A method for securely receiving a data message, comprising the steps of: obtaining a first decrypting key; generating a second decrypting key as a function of the first decrypting key and as a function of an identified parameter, wherein said identified parameter has a value; changing said value; and decrypting the data message using the second decrypting key to generate the data message.

10. The method of claim 9, wherein the decrypting step corresponds to a public key encryption scheme.

11. (Once Amended) The method of claim 10, wherein the [encryption scheme is] decrypting step corresponds to an RSA scheme.

12. The method of claim 9, wherein the decrypting step corresponds to a private key encryption scheme.

13. (Once Amended) The method of claim 12, wherein the [encryption scheme is] decrypting step corresponds to a DES scheme.

14. The method of claim 9, wherein the identified parameter is a time or time-dependent value.

15. The method of claim 9, wherein the identified parameter is a randomly generated number.

16. (Once Amended) The method of claim 9, wherein the [encrypted] data message is generated by a method comprising the steps of: obtaining a first encrypting key; generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter; encrypting the data message using the second encrypting key to generate an encrypted data message; and transmitting the encrypted data message.

17. (Once Amended) A communication system for securely transmitting a data message, comprising: a memory; a processor configured to execute the steps comprising: obtaining a first encrypting key; generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter, wherein said identified parameter has a value; changing said value; encrypting the data message using the second encrypting key to generate an encrypted data message; and a transmitter for transmitting the encrypted data message.

18. The communication system of claim 17, wherein the encrypting step corresponds to a public

key encryption scheme.

19. The communication system of claim 18, wherein the encryption scheme is an RSA scheme.

20. The communication system of claim 17, wherein the encrypting step corresponds to a private key encryption scheme.

21. The communication system of claim 20, wherein the encryption scheme is a DES scheme.

22. The communication system of claim 17, wherein the identified parameter is a time or time-dependent value.

23. The communication system of claim 17, wherein the identified parameter is a randomly generated number.

24. (Once Amended) The communication system of claim 17, further comprising a receiver configured to receive the encrypted data message and wherein a second processor is configured to execute the steps comprising: obtaining a first [decryption] decrypting key; generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter; and decrypting the encrypted data message using the second decrypting key to recover the data message.

25. (Once Amended) A communication system for securely receiving a data message, comprising: a memory; a receiver configured to receive an encrypted data message; and a processor configured to execute the steps comprising: obtaining a first decrypting key; generating a second decrypting key as a function of the first decrypting key and as a function of an identified parameter, wherein said identified parameter has a value; changing said value; and decrypting the data message using the second decrypting key to generate the data message.

26. The communication system of claim 25, wherein the decrypting step corresponds to a public key encryption scheme.

27. (Once Amended) The communication system of claim 26, wherein the [encryption scheme is] decrypting step corresponds to an RSA scheme.

28. The communication system of claim 25, wherein the decrypting step corresponds to a private key encryption scheme.

29. (Once Amended) The communication system of claim 28, wherein [encryption scheme is] decrypting step corresponds to a DES scheme.

30. The communication system of claim 25, wherein the identified parameter is a time or time-dependent value.

31. The communication system of claim 25, wherein the identified parameter is a randomly generated number.

32. (Once Amended) The communication system of claim 25, further comprising a transmitter configured to transmit the encrypted data message and wherein a second processor is configured to execute the steps comprising: obtaining a first encrypting key; generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter; and encrypting the data message using the second encrypting key to generate an [encrypted] data message.

33. (Once Amended) A method for securely transmitting a data message, comprising the steps of: obtaining a first array of encrypting keys; generating a second array of encrypting keys as a function of the first [encrypting key] array of encrypting keys and as a function of an identified parameter, wherein said identified parameter has a value; changing said value; encrypting the data message using the second array of encrypting keys to generate an encrypted data message; and transmitting the encrypted data message.

34. The method of claim 33, wherein the encrypting step corresponds to a public key encryption

scheme.

35. The method of claim 34, wherein the encryption scheme is an RSA scheme.

36. The method of claim 33, wherein the encrypting step corresponds to a private key encryption scheme.

37. The method of claim 36, wherein the encryption scheme is a DES scheme.

38. The method of claim 33, wherein the identified parameter is a time or time-dependent value.

39. The method of claim 33, wherein the identified parameter is a randomly generated number.

40. (Once Amended) The method of claim 33, further comprising: receiving the encrypted data message; obtaining a first array of [decryption] decrypting keys; generating a second array of decrypting keys as a function of the first [decrypting key] array of decrypting keys and as a function of the identified parameter; and decrypting the encrypted data message using the second array of decrypting keys to recover the data message.